



Overview of the UK Access Management Federation

Henry Hughes



Summary

- What is it?
- How does it work?
- Benefits
- What the service provides
- Suggested approach
- Further Information



The UK Federation

- A group of member organisations who sign up to a set of rules
- An independent body, managing the trust relationships between members
- End user organisations act as ‘identity providers’ (IdPs) and optionally ‘service providers’ (SPs)
- Publishers and resource providers act as ‘service providers’ (SPs)

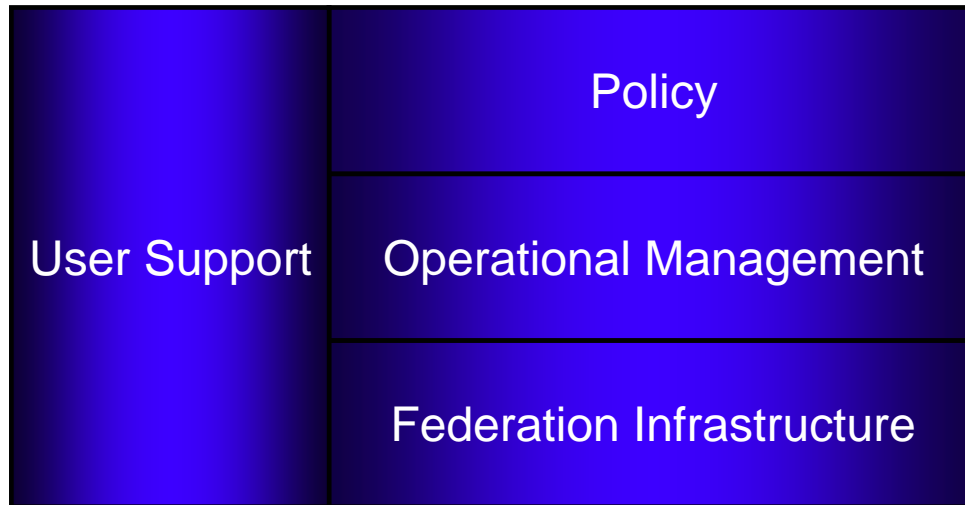


Organisational Structure

- Funded by Becta & JISC
- Provided for Schools, FE & HE
- Operational management by UKERNA
- Policy & Governance Board
- Technical Advisory Group

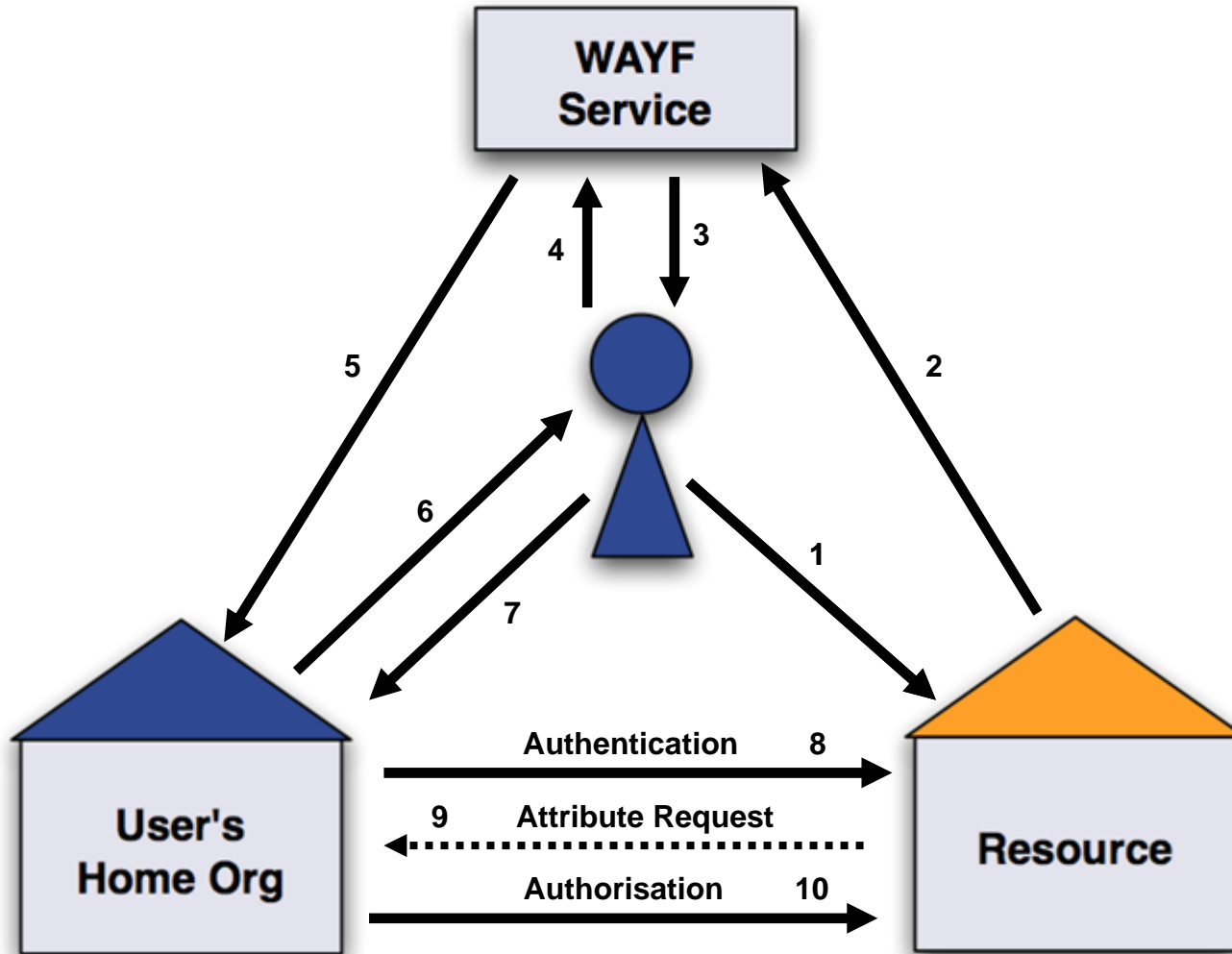


Components





How it works





Benefits

- Benefits for users
 - Much less need to disclose your identity
 - Personal data kept between you and your home organisation
 - Publishers can tailor services better
 - (At least) one less password to remember



Benefits

- Benefits for Identity providers (IdPs)
 - Typical IdPs are LAs, RBCs, FE, HE or Research
 - Easier to comply with regulatory requirements
 - Data Protection Act 1998, etc.
 - Better service offered to users
 - Uses existing access management systems
 - Can use same access control for all resources
 - Both internal and external
 - Fewer support problems



Benefits

- Benefits for Service providers (SPs)
 - Typical SPs are publishers, etc.
 - No need to maintain your own user database
 - Authentication is performed by the IdP
 - Can authorise per institution, role, and/or entitlement
 - Reduced user support requirements
 - Reduced compliance burden
 - Less storage/processing of personal data
 - Accurate implementation of licence conditions
 - Users take better care of credentials
 - Organisations take better care of assertions

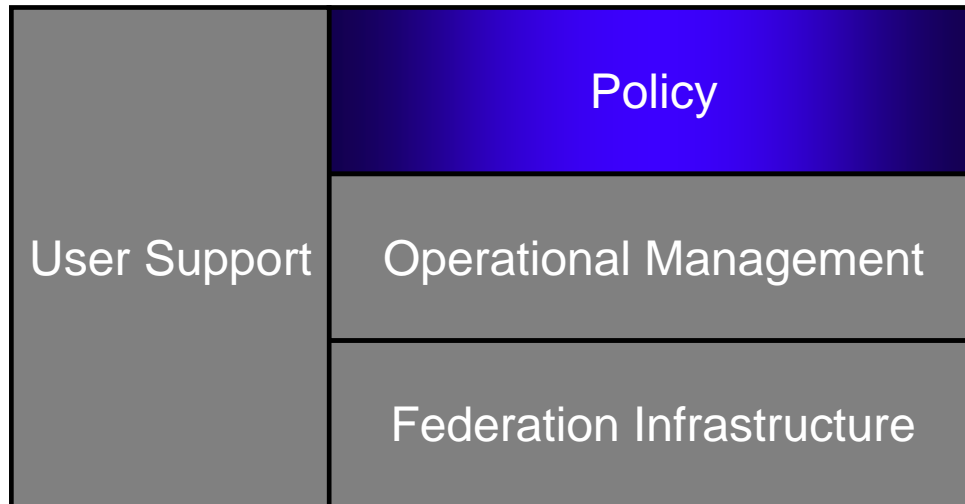


Benefits

- Benefits for the community
 - Provides consistency across the whole of education for federated (distributed) authentication and authorisation
 - Improves the user experience
 - Pooling of experience and expertise
 - Economies of scale for both sectors
 - Facilitates sharing of content and collaboration across sectors



What the service provides





What the service provides

- A set of Rules that binds members:
 - Make accurate statements to other members
 - If you say you can hold users accountable, do so
 - Keep federation systems and data secure
 - Use personal data correctly (inc. DPA1998)
 - Resolve problems within the Federation
 - Not by legal action
 - Assist Federation Operator and other members



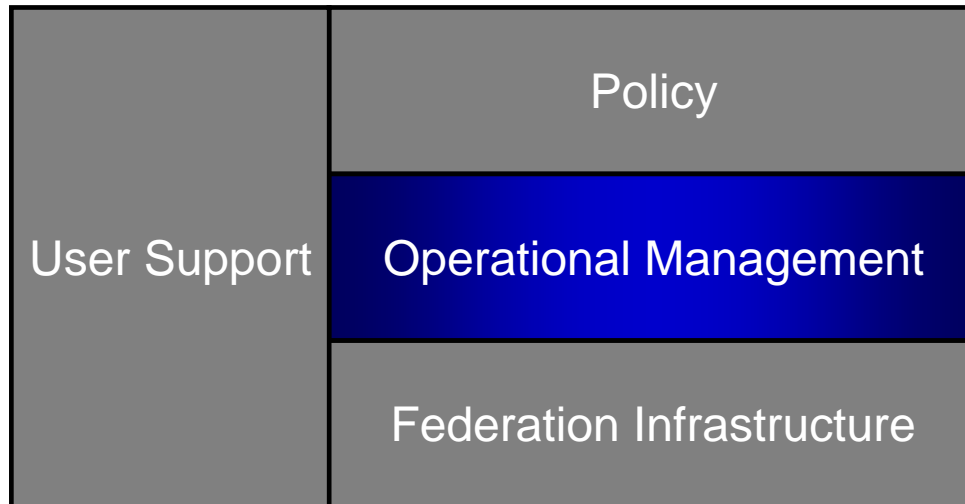
What the service provides

Guidance, examples, support

- How to comply with the Rules
- How to interoperate with other members
 - Common definitions, etc.
- Help in planning the transition
- Experiences of early adopters
- Software to implement Federation services
- All this is advisory, not prescriptive
 - Can use as much or as little as you need



What the service provides



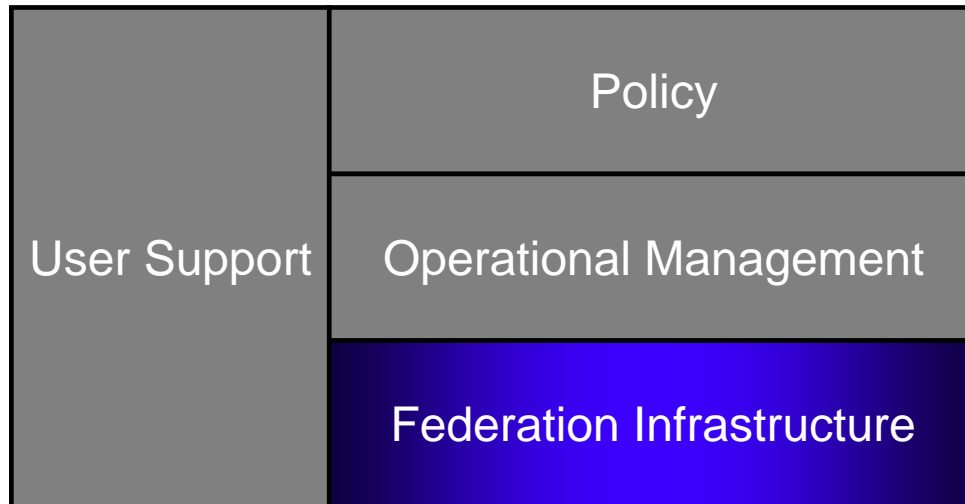


What the service provides

- Operational management
 - Registration mechanism for SPs and IdPs
 - Adding new members to the federation & updating existing members' metadata
 - Fault finding and trouble shooting
 - Compatibility testing of server certificates and CA Qualification
 - Technical and operational documentation
 - Ongoing federation development
 - Reporting



What the service provides



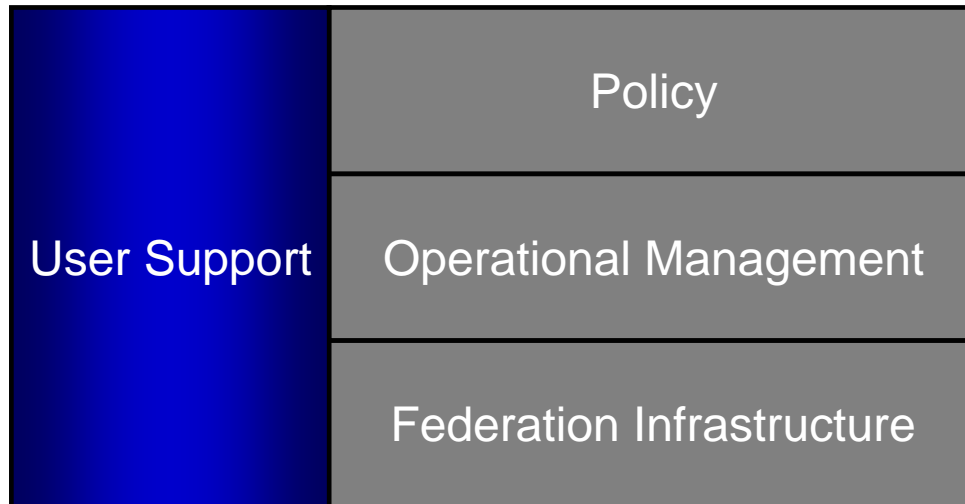


What the service provides

- Federation infrastructure
 - Discovery Service
 - Resilient WAYF
 - Hosting of metadata
 - Describes the Federation
 - Monitoring of SPs and IdPs
 - Test environment
 - Federation web site



What the service provides





What the service provides

- User support
 - Guidance and advice to IdPs & SPs
 - Configuration guides
 - Training courses
 - Online training material
 - Workshops to help organisations join the UK Federation
 - Frequently Asked Questions list



Suggested approach

1. LA/RBC audit - Review readiness to adopt federated access management.
2. Directory Development - Identify or implement a suitable local/regional directory.
3. Authentication Development - Choose and implement a local/regional authentication, or single sign-on system.
4. Implement IdP - Implement Identity Provider software.
5. Join Federation - All organisations who wish to participate will need to join the UK federation by registering and agreeing to observe federation policy.
6. Organisational Roll-out - On becoming a member of the federation, the organisation/LA/RBC will need to roll out the new system.



Further Information

- Website
 - www.ukfederation.org.uk
- E-mail lists
 - Ukfederation-announce@jiscmail.ac.uk
 - Ukfederation-discuss@jiscmail.ac.uk



Questions?